PRIVACY IMPACT ASSESSMENT (PIA)
CIO G6 Army Knowledge Online (AKO)

1. **Department of Defense Component:**

U.S. Army, Chief Information Officer

2. **Name of Information Technology System:**

Army Knowledge Online – SIPRNet (AKO-S)

3. **Budget System Identification Number (SNAP-IT Initiative Number):**

9990

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):**

2613

5. **IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):**

N/A

6. **Privacy Act System of Records Notice Identifier:**

AO025-1 CIO G6 Army Knowledge Online (AKO) Information System Records

7. **OMB Information Collection Requirement Number and Expiration Date:**

N/A

8. **Type of authority to collect information (statutory or otherwise):**

AKO authority to collect information is given by the following: E.O. 9397(SSN); Department of Defense Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance; and 10 U.S.C. 3013, Secretary of the Army.

10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance; and E.O. 9397(SSN).

9. **Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).**

The purpose of AKO is to perform knowledge management and register users in order to facilitate electronic communications and collaboration among DoD personnel and other authorized guest users. This system serves as an Army controlled repository for information needed by DoD personnel necessary for performance of duties and other DoD-related functions. Access is controlled based on individual needs for specific types of information. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation, or reporting purposes.

10. Identifiable Information to be Collected, its Nature and Source:

The AKO Lightweight Directory Access Protocol Data Store (LDAP) & Electronic Data Dictionary (EDD) includes the following primary personal information: individual's name, operator's/user's identification, SSN, birth date; email address, organizational address, telephone and fax numbers; military rank/grade, military branch, military MOS, assigned password (hashed), account types the source of this information is directly from the individual record subject and Army personnel and security database systems.

11. Method of Information Collection:

Personal information is provided by authoritative sources DEERS, ITAPDB and DMDC for non army personnel in support of DKO.

12. Purpose of Collection and How Identifiable Information/Data will be used:

AKO collects PII for authentication, access control to the system and information contained inthe system, and general ID management.

13. Does system create new data about individuals through aggregation?
This system does not create new PII about individuals through aggregation.

14. Internal and External Information/Data Sharing:

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Internal DoD agencies that would obtain access to Personally Identifiable Information (PII) in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Defense Manpower Data Center, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial

Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

15. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted:

A Privacy Act Statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and each time the user logs on to the system. System use and registration and use are voluntary and individuals choose to enter their own PII.

16. Information Provided to the Individual, the Format, and the Means of Delivery:

A Privacy Act Statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and each time the user logs on to the system. System use and registration and use are voluntary and individuals choose to enter their own PII.

17. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

System data is protected at the Secret level. All personnel accessing government computer information are required to undergo and receive at the minimum a favorable National Agency Check. The users include Active Duty Military, Federal Civil Service personnel and authorized contractors throughout the Army that have a need to know in order to perform official government duties. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment. The System Administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Currently, only system users and service liaisons (and their authorized contract users) have the capability to connect to the system. With the exception of Systems Administrators, Information Assurance Security Officers and software maintenance personnel, users fall into non-sensitive Information Technology (IT) Category III (non-privileged) positions as designated in DoD Directive 8500.1. Persons in IT Category-III positions require a National Agency Check, Entrance National Agency Check, or National Agency Check with Inquiries. All system administrators, information assurance and software maintenance personnel are in non-sensitive IT Category-I (privileged) positions. Persons in IT Category-I positions require a Single Scope Background Investigation (SSBI). Information is made available to users through the application or Enterprise server. Each authorized user must enter an appropriate User/Identification and Password before being authorized access to the resources. There is daily monitoring, daily notification of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). Files transferred across the SIPRNet do not leave the Army domain and are encrypted.

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures:

There are no risks in providing an individual the opportunity to object or consent or in notifying individuals. Appropriate safeguards are in place for the collection, use, and sharing of information. Security measures are adequate and the risk to AKO-S is minimal. Information is protected by user passwords, firewalls, antivirus software, and CAC access.

19. Classification and Publication of Privacy Impact Assessment:

Some data in this system is classified up to the secret level. This PIA may be published in full.